RBAC controlled computer system. Furthermore, the present invention is able to evaluate access grant dynamically (i.e., at runtime, potentially changing throughout the duration of the session) based on constraints with respect to each and every combination of subject information, object information, and environment information.

[0017] For present purposes, within an RBAC system, there is information subdivided into two kinds of information: content and context; and three categories of information, namely: subject, e.g., user, information, object, e.g., document, information, and environment or all other information.

[0018] Of the two kinds of information, content is per se factual information and context is the relationship between a plurality of facts. Content can be gathered by the present invention from two sources, namely: internal, that is, available within the controlled computer system and external, that is, available outside of the controlled computer system.

[0019] The present invention utilizes data extraction, such as by information retrieval, data mining, or natural language processing techniques, to obtain more data, i.e., content or context, or both, than is available from the controlled computer system. With the larger amount of data, sometimes referred to herein as "full" data, the present invention can determine and use more context to create a wide variety of constraint considerations. With full context, the present invention can enable constraints to dynamically change a grant of access, i.e., essentially anytime within a session or request up to the decision point (runtime) of access grant.

[0020] For the three categories of information, full data retrieval for the subject category enables more data related to the user to be retrieved, e.g., who the subject is and who might be related to the subject such as parents or co-workers. Full data retrieval for the object category enables more data or metadata related to the object to be retrieved, e.g., content within, or ownership of, a record. Full data retrieval for the environment category enables more data not in the subject or object categories to be retrieved, e.g., recognized disease symptoms. Application of suitable data extraction techniques, e.g., information retrieval, data mining, or natural language processing, to accomplish the present invention is assumed to be within the ordinary skill of the art.

[0021] Thus, the larger amount of data may enable more sophisticated permission-granting rules to be established, such as contexts entirely within a category, e.g., family relationship contexts or working personnel relationships. These contexts may be established based on external data gathered about a subject. By also enabling data extraction internal to the controlled computer system, the present invention can also enhance the content available to set the constraints by extracting and evaluating object content based upon the actual data, and not just metadata, within the object requested. Also, increasingly sophisticated contexts between two categories may be had. For example, a so-called "application context" based upon both subject information, including assigned role(s), and object information, such as the relationship between the user and the data being accessed, may be attained. Also a so-called "system context" based on environment information and subject information, such as the relationship between a time window in which the object request is critical and the identity or role of a subject entitled to the critical information, may be attained. For instance, in a process of a complicated surgery, an anesthesiologist may need to obtain the genetic makeup of the patient but is allowed access to such data only at the time that the anesthesiologist needs to administer certain types of medication.

[0022] To further provide increased utility for RBAC systems, the present invention, by utilizing full content and full context, can enable dynamically changing access to objects, i.e., dynamic change of constraints and application of the permission-granting rules for a given role immediately before the run-time of every access determination. (All prior RBAC systems are believed to provide only static capabilities, i.e., access rights of a role remain constant throughout a session once the role of the subject is determined.) For example, access may change dynamically on a request-by-request basis, even within the same session, depending on potential environmental conditions, such as system context based on environment information (and subject information) such as in the above example where the elapsed effective time of an anesthetic may determine the urgency of an access request and thereby change the access permissions of the Anesthesiologist role.

[0023] By enabling extraction of subject, object, and environment content from internal and external sources, the present invention can utilize as much content and determine as much context as is necessary for refined and dynamic permission constraint writing, thereby enabling system administrators to easily write fine grained permission constraints necessary for proper access control to objects within a role-based access control system on an "as-needed" basis.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0024] The objects and features of this invention will be better understood from the following detailed description taken in conjunction with the drawings wherein:

[0025] **FIG. 1** is a schematic of an RBAC system with role permission capability as known in the art.

[0026] **FIG. 2** is a schematic of an RBAC system and method according to the present invention with refined and dynamic permission constraint capability.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0027] The exemplary embodiment of an RBAC system will be set forth in the context of a medical records access control system. Medical domains are challenging because, for example, of the complex relationships among medical personnel (subjects/users) within an organization, and the complex relationships among patients and caregivers and other users of the controlled computer system which may have some relationships with the patient. The medical records (objects) are also complex in their contents and may contain data related only by the fact that it has occurred in the same patient/owner of the record. Further, complex rules for granting or restricting access to the electronic records now occur and are enforceable by law. Further, granting timely and appropriate (e.g., using environment content and context) access to the records for the appropriate personnel may be critical to patients' lives.

[0028] Discussion of the modules of the exemplary RBAC method or system will be given herein with respect to